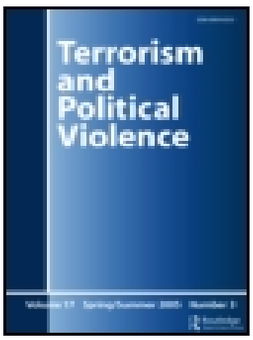

Terrorism and Political Violence

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ftpv20

An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks

Thomas J. Holt , Jin Ree Lee , Joshua D. Freilich , Steven M. Chermak , Johannes M. Bauer , Ruth Shillair & Arun Ross

To cite this article: Thomas J. Holt , Jin Ree Lee , Joshua D. Freilich , Steven M. Chermak , Johannes M. Bauer , Ruth Shillair & Arun Ross (2020): An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks, Terrorism and Political Violence, DOI: 10.1080/09546553.2020.1777987

To link to this article: https://doi.org/10.1080/09546553.2020.1777987

Published online: 26 Aug 2020.

TERRORISM AND POLITICAL VIOLENCE
https://doi.org/10.1080/09546553.2020.1777987

Routledge
Taylor & Francis Group

An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks

Thomas J. Holt[a], Jin Ree Lee[a], Joshua D. Freilich[b], Steven M. Chermak[a], Johannes M. Bauer[c], Ruth Shillair[c], and Arun Ross[d]

[a]School of Criminal Justice, Michigan State University, East Lansing, Michigan, USA; [b]Department of Criminal Justice, John Jay College—CUNY, New York, New York, USA; [c]Department of Media and Information, Michigan State University, East Lansing, Michigan, USA; [d]Department of Computer Science and Engineering, Michigan State University, East Lansing, Michigan, USA

ABSTRACT

Web defacement is a form of hacking that involves altering the content of a website, resulting in repairs to the website code, loss of revenue, internal loss of productivity, and reputational damage. Limited research has examined the frequency of web defacements, the factors that distinguish them from other hacking motives, and the extent to which the correlates mirror research on physical acts of ideologically-motivated crime. The current study examined over 2.4 million web defacements hosted in the U.S. from 2012 to 2016 to assess aspects of routine activities theory associated with target selection and attack methods among ideologically-motivated defacements. A binary logistic regression analysis revealed that ideologically-motivated defacers were more likely to use unknown vulnerabilities; engage in repeated attacks; target top-level domains linked to foreign nations; domains ending in.edu; and homepages within websites. The findings of this study suggest that the target selection process of ideologically-motivated defacers are more purposive and designed to draw attention to their cause, resembling target preferences of individuals who engage in physical violence in support of an ideological agenda.

KEYWORDS

Cybercrime; computer hacking; extremism; cyberterror; routine activities theory

Introduction

Research examining cybercrimes has increased dramatically over the past three decades, due in part to the near ubiquity of technology and societal dependence on the Internet and computers for all aspects of communication, finance, and governance.[1] A growing body of literature specifically focuses on cybercrimes that target computer networks and sensitive data, including computer hacking and malicious software attacks.[2] These offenses appear to be driven by instrumental motivations,[3] as attackers can generate substantial financial profits from access to sensitive personal and financial information.[4]

Far less research has considered the potential use of the same cyberattack methods to further ideological motivations, such as political, nationalist, religious, or other belief-based reasons.[5] Some define such incidents as acts of cyberterror,[6] though this term has created intense debate over whether such attacks pose a true threat.[7] Regardless, law enforcement and government agencies recognize that ideologically motivated attackers may target any aspect of government and/or civilian-managed online critical infrastructure.[8] In fact, the Department of Homeland Security predicted that terrorist groups and extremists will increase their use of cyberattacks against the government and industry targets.[9]

CONTACT Thomas J. Holt holtt@msu.edu School of Criminal Justice, Michigan State University, East Lansing, MI 48824, USA.

Lack of access to information about these incidents is one of the main reasons for the absence of empirical research on ideologically motivated cyberattacks.[10] Similar to how businesses and government organizations provide minimal public reporting on cyberattacks affecting their infrastructure, it is unclear how often police become aware of these incidents.[11] Relatedly, cyberattacks are often omitted from the current slate of terrorism databases due to their failure to qualify as a "violent" incident.[12] In fact, ideologically motivated incidents are currently prosecuted under existing federal statutes related to cybercrime rather than terrorism-related charges.[13]

Consequently, limited research has examined the factors influencing these attacks and the commonalities between ideologically motivated cyberattacks and those performed for other instrumental or expressive motivations.[14] A form of cyberattack that allows analysis of these issues are web defacements. An attacker may use a range of attack methods to alter the content of a public-facing website to images, media, and text of the attacker's choosing.[15] Website defacements also produce economic costs for victims, including repairs to the website code, loss of revenue from any site downtime, internal loss of productivity costs, and reputational damage.[16]

Defacements occur with great frequency each year. They are performed for various reasons beyond their instrumental impact on their intended target.[17] Individuals report defacing sites to amuse themselves or demonstrate their skills in keeping with the broader motives reported among computer hackers.[18] A portion of defacers also perform these attacks in support of political, nationalist, or ideological beliefs.[19] For instance, attackers associated with the Animal Liberation Front,[20] ISIS,[21] and far-right ideologies have launched defacements against government and business sites across the U.S.[22]

Limited research has examined how ideologically-motivated defacements differ from those performed for other motives, particularly with respect to target selection in the course of the attack. Research on extremist violence in physical space suggests attackers purposively select targets that reflect their ideological beliefs.[23] The opportunity structure for online offending differs from real world violent crime as virtual spaces eliminate physical and geographic boundaries from targets.[24] At the same time, attackers may be limited on the basis of their technical skill, making it possible for more indiscriminate target selection depending on their motivation.[25] Thus, it is unclear if ideologically-motivated defacers' target selection and attack methods are distinct from those driven by different expressive motivations within the hacker subculture, such as a desire for social status or proving one's abilities.[26]

This exploratory study seeks to address this question through an analysis of over 2.4 million defacements reported against websites hosted in the U.S. from 2012 to 2016. A binary logistic regression model was estimated to test aspects of routine activities theory associated with target selection and attack methods among ideologically-motivated defacements.[27] This model extends prior research examining physical terror and extremist violence victims,[28] and provides direct implications for our understanding of the contours between cyberattacks and physical attacks generally.

Situating actor ideology in the context of web defacements

Web defacements are a common occurrence with millions happening each year. In fact, a recent estimate suggests that website defacements comprise about 19.7% of all online attacks each year.[29] Individuals who engage in defacements also tend to note their accomplishments publicly, through defacement archives, social media, and websites.[30] Defacers will even leave e-mail addresses and social media profile names on the pages they compromise so as to link their online identity to the incident.[31] The relatively overt, public nature of defacements makes defacers different from other hackers who seek to minimize attention to their exploits for fear of being detected or losing access to sensitive targets.[32]

Web defacements may be performed for a range of expressive motivations,[33] including ego development, social recognition from peers, entertainment, and to draw attention to political or social

causes.[34] Web defacements originally began as a vehicle for hackers to expose system administrators who used poor security protocols on their websites and servers, while generating a reputation as a skilled individual in the hacker community.[35] Individuals still engage in web defacements for these reasons, particularly those who are relatively new to the hacker subculture. Broadcasting hacks to the public which can be linked to the defacers' handle, or online identity, helps to demonstrate their mastery of computer skills.[36] Similarly, defacements can be performed for the sake of fun and laughs because of system administrators' weak security, or one's ability to identify weaknesses in servers or webpages.[37]

Defacers are not solely motivated by subcultural beliefs, as they may be willing to attack any target so long as it can be situationally justified by their own personal history. Defacers may also choose to engage in attacks that reflect personal beliefs and expericnes due to situational and foreground dynamics, such as their national identity or religion.[38] The expressive nature of defacements make them innately valuable as tools that promote political and/or social beliefs, whether through the language used in the defacement or the target of the attack. Such attacks may be referred to by some as "hacktivism" or the expression of activist principals through hacking behaviors.[39]

Evidence suggests defacements typically increase in the wake of real world events that provoke political or ideological responses from affected populations.[40] For example, one of the earliest website defacements targeted the U.S. Central Intelligence Agency's (CIA) website and was attributed to Swedish hackers protesting the prosecution of their fellow hackers for actions they took against a telecommunications company.[41] More pointed political defacements occurred in the early 2000s as access to computers and the Internet spread across the globe, enabling attackers' access to targets in any nation.[42] This was exemplified by a series of defacements performed between Chinese and U.S. hackers after an American EP-3 reconnaissance plane collided with a Chinese F-8 fighter jet over Chinese airspace in April 2001. The Chinese pilot died during the incident and the U.S. flight crew was detained following an emergency landing.[43] Media coverage of the incident generated a massive series of defacements against U.S. and Chinese websites in an attempt to express patriotic attitudes and support for the attackers' home nation.[44]

Turkish hackers began a similar campaign of web defacements after the publication of twelve cartoons depicting the prophet Mohammed in the Danish paper *Jyllands-Posten*.[45] The defacements were conducted by actors claiming to support the Muslim faith and express outrage over the way their spiritual leader was being portrayed in popular media. A number of defacement campaigns have also been exhibited by actors aligned with far-left extremist groups against industrial and governmental targets in an attempt to embarrass and shame their victims for harming both animals and the environment.[46] Several far-right actors have also been implicated in defacements targeting websites serving Holocaust memorial sites over the last decade.[47]

Differentiating ideologically motivated cyberattacks

The situational variations observed in the motives of defacers calls to question whether web defacements performed for ideological reasons differ from those that reflect the values of the hacker subculture, such as entertainment or demontrations of skill.[48] Research comparing extremist violence to other forms of violence may provide insight as to the ways ideological web defacements operate. For instance, some terrorism studies maintain that victims of ideologically motivated attacks are randomly selected.[49] In contrast, research using inferential statistics demonstrates that most victims of ideologically-motivated violence in the real world are not random, but targeted for either purposive or symbolic value reflective of the group's ideological agenda.[50] Perpetrators are more likely to target individuals based on characteristics such as race, sexual orientation, government affiliation, and occupation because of both visibility and frequency in population.[51]

Additionally, the extant literature on homicide suggests that ideologically motivated attackers do not personally know their victims. This is in stark contrast to non-ideologically motivated violence, as research indicates that non-ideological victims and offenders are strangers 22.9% of the time,

acquaintances 57%, and family members 20.1%.[52] Most ideological victims are targeted because of what they represent to the offender, making it uncommon for both parties to have personal relationships prior to the incident.[53] In instances where the victim and offender have a prior relationship, it is often out of circumstance rather than strong social bonds.[54]

Given the dearth of research on ideologically motivated cyberattacks, it is unclear whether the relationships observed in offline ideologically motivated violence are also present within the online context. Physical attacks require terrorists or extremist groups to converge with their target in time and space as demonstrated by routine activity theory.[55] Specifically, the theory argues that for crime to occur, offenders and suitable targets must converge in time and space in the absence of guardians who could shield the target from harm. As a consequence, the behaviors of victims and offenders create various predictable patterns of geospatial interaction.[56]

Some have argued that a spatio-temporal convergence is less feasible in virtual space as the Internet renders an attacker equidistant to their target regardless of their location in physical space.[57] Additionally, the Internet as a resource is always available, making targets accessible to potential offenders at all times.[58] Despite these criticisms, the basic tenets of the theory have been supported in studies examining various forms of cybercrime victimization, including online harassment,[59] hacking,[60] malware infections,[61] and fraud.[62]

In terms of routine activity theory and web defacements, an attacker's perception of target suitability and attractiveness may be influenced by a website's various qualities and characteristics.[63] Defacers motivated by an ideological or political cause may be more likely to target specific sites relative to those driven by other subcultural values or motives.[64] For instance, the value of a target may be tied in part to its URL, since it can resolve to a representation of physical spaces through Top Level Domains (TLD). The ending component of a URL may resolve to a country (e.g., .cn, .nl, .uk), though the actual physical location where the site is hosted may differ due to disparities in technological infrastructure by country.[65] In fact, many websites hosted in the U. S. resolve to a domain for a different country, such as .br, .in, and others.[66] As a result, the TLD of a website may influence its value for ideologically motivated defacers who seek to target a specific nation in opposition to its policies or practices.[67]

It is also possible that ideologically-motivated defacers may be more likely to target high profile websites, especially those run by governments, businesses, and organizations whose interests run contrary to those of the actor(s).[68] Such actions would correspond in part to physical terror and extremist violence, which target infrastructure and persons who symbolically represent their ideological beliefs.[69] The relatively low risk of detection from formal law enforcement agencies in online spaces may also reduce the perceived risk of targeting high visibility organizations like a government or military website.[70] Thus, it is sensible that ideologically motivated actors may be more likely to target domains indicative of government (.gov), military (.mil), or educational (.edu) targets online compared to all other motivations.

An additional factor that may influence the potential value of a website is its inertia, or its relative size.[71] A single web server can host as few as one website or dozens of sites, each with multiple pages depending on its storage capacity. A defacement that targets all pages hosted on a server would be referred to as a mass defacement and may demand a higher degree of technical skill to complete due to the effort required to affect a target with greater inertia.[72] In this respect, a mass defacement may be similar to the notion of targeting a building or aircraft with a bomb in acts of ideological violence within physical spaces.[73] Such attacks are infrequent in physical spaces compared to traditional acts of interpersonal violence performed by ideologically motivated actors.[74] In sum, individuals interested in defacing sites in support of an ideological cause should be willing to target any resource of convenience to promote their beliefs in lieu of mass defacements, including a single page within a site.

The accessibility of the target may also influence the likelihood a defacement is ideologically-motivated, particularly the operating system of the web server that hosts the site. Web servers are a form of computer hardware that requires a specialized operating system (OS) in order to process and manage information.[75] The OS of a server is similar to that of desktop or laptop software as it enables

the system administrator to configure and manage both the hosted content and users' behavior. There are two types of OS: "open source" and proprietary or "closed source." The program code of open source software is publicly accessible, enabling users to identify and publicly report flaws in code that could be used to compromise the system.[76] The second form is sometimes called "closed source" software, such as Microsoft Windows and Apple iOS, because these companies limit access to their source code, thereby limiting vulnerability reporting and slowing the production of security updates to repair the code.[77]

Since most web servers utilize open source software, such as Apache,[78] their flaws may be more visible and accessible to the attacker community, making them a greater opportunistic target for attack.[79] While attackers motivated by showing off their hacking skills might be influenced by a server's OS, ideologically motivated defacers may not be swayed by the convenience with which they can affect a target. Instead, they may be more likely to target sites on the basis of other extrinsic and intrinsic factors.[80] As such, it is hypothesized that the OS of a target is not related to its likelihood of being compromised by ideologically motivated defacers.

Attackers may also select to deface specific portions of websites based on their accessibility to the attacker and visibility to the public. The homepage, or main landing page of a website, should generate higher visibility to the general public compared to secondary pages within the site.[81] The homepage of a website may also be more secured than secondary pages due to its perceived visibility and risk associated with that content.[82] Since ideologically motivated defacers seek to generate attention to their cause, they should be more likely to target homepages within websites rather than secondary pages contingent on the security of the page.

Since websites are always available online, their visibility and accessibility may increase the risk of repeat victimization from defacers, particularly those driven by ideological motives. Specifically, those motivated by ideology may be more likely to engage in repeat defacements of the same sites due to the potential that they operate in contrast to their beliefs or cause harm to a certain group.[83] The recognition that a target can be compromised may also increase its potential attractiveness for ideologically motivated actors as they may want to ensure their attack is successful.[84] Thus, a website should be more likely to be repeatedly targeted by ideologically motivated actors.

Finally, defacers' method of attack may also be associated with their ability to access a specific target.[85] Web defacers can utilize multiple attack methods to complete a strike, ranging from simple password guessing to the use of scripts and vulnerabilities that can be exploited within the server's OS.[86] The use of various tactics to affect a target is similar to acts of physical violence, which can include simple assaults to bombings.[87] Evidence suggests that terrorists and extremists prefer to use simple, accessible, and easy-to-use weapons to ensure successful outcomes against physical targets.[88]

There is limited research examining this issue relative to the motivation of a hacker, though an individual's knowledge of computer hacking may limit their capacity to complete certain forms of attack.[89] Most hacks, including defacements, involve compromising a computer system by exploiting the presence of a vulnerability, or flaw, in the software of the targed system.[90] There are two types of vulnerabilities: "unknown" and "known." In the case of unknown vulnerabilities, the flaw has been identified by an attacker but not yet reported to the software manufacturer.[91] Such vulnerabilities are difficult to defend against, as there is no known security fix available at that time. An attacker using such a vulnerability is also likely to have more technical sophistication, as they are likely to have determined where the vulnerability is present, and created a unique program that enables them to utilize the flaw in an attack.[92]

Eventually, most unknown vulnerabilities become known, suggesting the original flaw has been reported to the software producer.[93] The company then produces security patches that can be downloaded to update the system and keep attackers from using it to gain access. Not every computer system will, however, implement patches that decrease their likelihood of being compromised.[94] In this respect, the use of known vulnerabilities may be associated with semi-skilled attackers as they may be able to utilize existing, pre-written attack programs to compromise vulnerable systems.[95] In fact,

a number of attack tools available for download include exploitable code for known vulnerabilities so as to facilitate attacks by lower-skilled cyberattackers.[96]

Though limited research has explored the issue of technical proficiency among ideological actors, it may be that they have lower levels of expertise than those who hack in order to demonstrate their mastery of technology.[97] For instance, there is evidence that some Turkish web defacers use an attack method called SQL injection, where an attacker exploits a well-known weakness in database software to gain access to the site.[98] At the same time, attackers seeking to affect high-value targets like government or military websites may have to utilize less common vulnerabilities in order to be effective.[99] Thus, ideologically motivated attackers should be more likely to use unknown vulnerabilities in order to increase their likelihood of success compared to those who hack for more intrinsic, ego-centric motivations.

The present study

Taken as a whole, web defacements comprise a distinct form of cybercrime that can be performed for any number of expressive motives.[100] One key motive of defacers appears to be ideological or political in nature, as cyberattacks provide a high-visibility tool for attackers to express their political, social, or religious beliefs.[101] There is limited research examining the frequency of such defacements, the factors that distinguish them from other hacking motives, and the extent to which the correlates may mirror research on physical acts of ideologically-motivated crime.

The current study attempted to address this gap in the literature through a quantitative analysis of all web defacements self-reported by attackers against websites within the U.S. web space. This study examined multiple hypotheses considering the relationship between targeting decisions and motivation. First, this study analyzed whether ideologically motivated attackers were more likely to target top level domains for countries outside the U.S. and high-profile domains, such as government and educational sites, as a function of the perceived value of their desired target. Second, this study tested the hypothesis that ideologically motivated actors may engage in single page defacements rather than mass defacements as a function of the perceived inertia of the target. Third, this study tested various aspects of the accessibility of a target relative to attacker motivation. Specifically, it is expected that ideological defacers would target servers regardless of their OS, but target homepages of websites, engage in repeated attacks against a target, and use unknown vulnerabilities in order to be successful. The findings and implications of this analysis for our understanding of the relationship between physical and virtual ideologically-motivated attacks are discussed in detail.

Data and methods

Similar to terrorism research, studies exploring cyberattacks face challenges in accessing primary data.[102] There are few official data sources that provide a comprehensive enumeration of computer-focused offenses such as hacking.[103] Industry or open-source government resources are rarely available due to underreporting on the part of victims, particularly within private industry over fears of economic loss and a decrease in consumer confidence.[104] Cybercrime scholars have utilized a variety of open source and novel data collection strategies to empirically assess hidden forms of crime, such as hacking and malware.[105]

Web defacements are one of few highly visible forms of computer hacking due to the publicly accessible nature of websites and attackers' interest in publicizing their skills.[106] There is an existing repository of data related to website defacements in the archive maintained by the website "Zone-H."[107] This website has been active in various forms for more than a decade, providing an outlet for hackers who engage in web defacements to publicly report and/or advertise websites they have defaced.[108] The repository is similar to the self-claiming strategies that terror and extremist groups employ online to attribute physical attacks to their members.[109] In fact, tens of thousands of

defacements are reported, verified, and noted in their archive, making it a relatively comprehensive data source for research on defacements.[110]

When a malicious online actor engages in a defacement, they can report their actions to the Zone-H website through an online form where they are asked to provide a hacker handle (i.e., adopted online identity of the individual or group) that is labeled as the "notifier" for the defacement. Respondents are also asked to provide some characteristics about the web defacement. For instance, notifiers often indicate the web domain affected (including the date and time), their nickname, the method used to engage in the defacement through a dropdown menu, and the rationale for the attack. The information is passed along to Zone-H site administrators who validate the claims and, if accurate, archive the defacement so that it can be mirrored in perpetuity on their site.

To develop a purposive sample of defacements, the researchers selected to focus on all IP addresses hosted within the U.S. due to its global involvement in myriad political and social conflicts, as well as it being one of the largest providers of web hosting services for countries around the world. These characteristics make U.S. websites a potential target for political and ideologically motivated actors globally.

Zone-H allows the public to see only the last 600 defacements that were reported and validated through their site, limiting the overall information that may be observed. In order to assess a wider range of political and social events that may have impacted the potential for defacements, the research team contacted Zone-H to gain access to all defacements reported to the site between January 1, 2012 and December 31, 2016. The team was given access to all 2,285,256 total defacements reported to the site during this period, regardless of actor motivation. Similar to studies comparing ideological violence to other forms of violence, this provided the research team with a large sample of incidents to compare those ideologically and/or politically motivated defacements against all others reported by attackers.[111]

Dependent variables

The dependent variable for this analysis was the attackers' self-reported motivations for carrying out a defacement. Zone-H data allows the reporting attacker to indicate their reason for performing the defacement from a series of six options: (1) just for fun, (2) as a challenge, (3) to be the best defacer, (4) patriotism, (5) political reasons, and (6) revenge against that website. In the event the attacker does not want to report a motivation, Zone-H scores their response as "not available," creating a seventh category. Only one response could be provided at a time, making each incident associated with a specific motive. The majority of incidents were reported as being performed for fun (51.1%), to be the best (21.5%), and for a challenge (4.7%) which are common reasons for hacking generally.[112] A small proportion of incidents were performed for an unspecified reason (9.1%), as well as for revenge (4.6%). Patriotism (3.2%) and political (5.7%) motivations were less common, though present and persistent at the same levels in every year.

The use of a reporting mechanism that allows the respondent to select only one motive limited our ability to assess the full scope of an attacker's situational decision-making to assign one motive over another to their attack.[113] While self-described "patriotic" and "political" hackers may differ in their targeting preferences, both reflect ideological beliefs held by the attackers.[114] As such, these two measures were combined into a single, binary variable (8.9% total), forming the dependent variable for this analysis (0 = no; 1 = yes; see Table 1). This measure provided a way to assess the factors associated with self-identified ideologically motivated defacements compared to all other potential motives among relatively active and attention-seeking segments of the hacker subculture.

Independent variables

Five binary variables were created to measure factors associated with a target's potential value and attractiveness to the attacker. To assess the relationship between the potential value of a target based

Table 1. Descriptive statistics (n = 2,285,256, clustered by 29,229 attackers).

Variable	Mean	SD	Min	Max
Motives	0.089	0.000	0	1
Domain	0.246	0.000	0	1
.gov	0.004	0.000	0	1
.mil	0.0004	0.000	0	1
.edu	0.006	0.000	0	1
.org	0.067	0.000	0	1
Single Defacement	0.254	0.000	0	1
Server OS	0.187	0.000	0	1
Homepage	0.443	0.000	0	1
Redefaced	0.100	0.000	0	1
Unknown vuln	0.029	0.000 0	0	1
Known Vuln	0.159	0.000	0	1
SQL Injection	0.293	0.000	0	1

on its association to a specific country, a variable identifying whether the victim site resolves to a non-U. S. Top Level Domain (TLD), such as .br or .kr, was created (*domain*; 0 = no; 1 = yes). An additional set of four binary variables were included to explore associations between attacker motivation and target value based on the TLD of the defaced website within a specific U.S. context. These measures were created based on the target URL resolving to a site ending in: (1) .gov; (2) .mil; (3) .edu; and (4) .org (0 = no; 1 = yes). Each of these domains may have greater value due to their relation to either governments, academic institutions, or independent organizations which may reflect an ideological preference on the part of the attacker.

To assess the role of inertia in target selection, a variable was created to capture if the attacker engaged in a mass defacement where they simultaneously defaced as many pages hosted on a server as possible, or whether a single page within a site on a server was attacked (0 = mass defacement; 1 = single defacement). *Single defacements* may reflect an attacker's interest in affecting a target of convenience which has less inertia or mass.

To assess factors associated with target accessibility, six binary measures were created. First, a measure was produced to reflect the OS of the server *(serverOS)* on the basis of open and closed source programs. As discussed above, open source programs may be more easily compromised than closed source programs due to the public reporting and patching processes used by open platforms such as Linux.[115] The majority of servers in this sample utilized some variation of the Linux OS (81.3%), with the remainder running either Macintosh, Microsoft, or Unix-based programs. Thus, non-Linux systems were combined into a single measure (0 = Linux; 1 = non-Linux) as these programs reflect a smaller proportion of all server systems as a whole.

A measure was also included to capture whether the attacker targeted the *homepage* of a website or a secondary page (0 = secondary; 1 = homepage). Homepages may generate greater attention for the attacker as they would be immediately visible to anyone visiting that URL, though secondary pages may be less secured, enabling greater ease of access. An additional measure assessed whether the target was *redefaced* (0 = no; 1 = yes), meaning it was attacked once or multiple times by different attackers. It is possible that ideological attackers may be more likely to engage in redefacements due to their ability to affect the same target and constantly draw attention to an issue or political statement.

Finally, three measures were included to examine any relationship between the use of specific attack methods by an actor and their motivation. A binary measure was created for attackers' use of (1) unknown vulnerabilities (*unknown vuln)*; (2) known vulnerabilities (*known vuln)*; and (3) *SQL injection* (0 = no; 1 = yes). The use of undisclosed vulnerabilities within a server or OS platform should be associated with attackers who have either a greater degree of technical proficiency or access to knowledgeable attackers. Those using known vulnerabilities to attack were also likely to have a degree of technical proficiency but used more common or known methods. SQL injection attacks were, however, more common and anecdotally associated with ideologically motivated defacers like those in the Turkish hacker community.[116]

Results

To examine the relationships between attacker motivation and target characteristics of the defacement, a binary regression model was estimated (see Table 2). There was no evidence of multicollinearity as the lowest tolerance was .535 across all models and the highest Variance Inflation Factor (VIF) was 1.987. Due to the very large number of defacements in the data set, the assumption of independent observations was violated which would lead to an underestimation of the standard errors when not appropriately corrected for. Thus, the analysis were conducted using STATA statistical software using the cluster command by attacker to compute robust standard errors.

The findings demonstrate that ideologically motivated defacers were more likely to target systems based on certain characteristics compared to all other defacers.[117] First, ideologically-motivated defacers were more likely to target sites whose TLDs resolved to different nations (see Table 2). Additionally, those domains ending in .edu were more likely to be targeted by defacers, suggesting some association between target value and general web extension. There was, however, no support for the hypothesis that defacers would be more likely to engage in single defacements compared to mass defacements as this variable was non-significant.

A positive relationship between target accessibility and ideological defacements was also supported. Ideologically motivated attackers were more likely to deface homepages rather than secondary pages within a site. No relationship between the OS of a target and ideological defacements was found. Additionally, ideologically-motivated defacers were significantly more likely to engage in redefacements of targets. In terms of the attack methodology, defacers were more likely to use unknown vulnerabilities to complete attacks compared to all other defacer motivations. In addition, ideologically motivated defacers were significantly less likely to use known vulnerabilities and SQL attacks.

Discussion and conclusion

Although there is a substantial body of research regarding physical acts of violence motivated by ideology and extremism, there is far less research considering the scope of online ideological attacks. This study sought to examine the relationship between target selection of web defacements for ideological motivations relative to those of the larger hacker subuclture using hypotheses derived from routine activity theory. The current study used a sample of over 2.4 million defacements reported against websites hosted in the U.S. from 2012 to 2016 to examine attackers' targeting decisions and the extent to which they may mirror target selection in acts of physical violence for ideological reasons.[118]

The findings demonstrated some commonality between these behaviors, while also finding partial support for routine activity theory.[119] As hypothesized, the study found that ideologically motivated

Table 2. Regression model (n = 2,285,256, clustered by 29,229 attackers).

Variable	b	SE	ExpB
Domain	0.142	0.054	1.152**
.gov	0.031	0.228	1.031
.mil	−0.044	0.150	0.9561
.edu	0.364	0.146	1.439**
.org	−0.005	0.043	0.994
Single Defacement	0.130	0.084	1.139
Server OS	−0.164	0.169	0.847
Homepage	0.599	0.128	1.820***
Redefaced	0.099	0.051	1.105*
Unknown vuln	0.486	0.222	1.626**
Known Vuln	−1.659	0.181	0.190***
SQL Injection	−0.438	0.205	0.645**
Constant	−2.429	0.141	0.088***

*p < .05; **p < .01; ***p < .001, Chi = 50087.03***; Psuedo R^2 = .045; −2LL = − 656577.18.

defacers were more likely to target systems based on specific characteristics of the site itself. For one, ideological defacers were more likely to target sites whose TLDs were linked to nations outside of the United States. This finding suggests target selection is a function of its value to the attacker based on their political or patriotic causes and the scope of nations' whose online content is hosted within the U.S. The study also found that domains ending in .edu were more likely to be targeted by ideologically motivated defacers.[120] These findings are similar to studies of ideologically-motivated physical violence which find victims are not random but targeted for either purposive or symbolic value reflective of the group's ideological agenda.[121]

There was, however, no significant relationship observed between ideological defacements and targeting sites with military (.mil), government (.gov), and organizational (.org) website extensions. In theory, the relatively low risk of detection from formal law enforcement agencies in online spaces should have reduced the perceived risk of targeting high visibility organizations across the spectrum.[122] Research suggests cyberattacks that are associated with far-left extremist groups target government, industry, and educational institutions.[123] The lack of significance observed here may reflect differences in the potential accessibility of these sites, as they may be more difficult targets to compromise compared to those operated by educational institutions. Future research would benefit from considering unique factors that shape risk of attack on the basis of a target's domain relative to its actual content.

Additionally, this study found no relationship between the inertia of a server as a target for ideologically-motivated defacement. It was hypothesized that single pages would be more likely to be defaced by ideological attackers as a point of convenience rather than attempts to engage in mass defacements to affect all pages within a server. The lack of support for this hypothesis suggests inertia may be less relevant for web defacements compared to weight and size in acts of physical violence performed by ideological actors.[124] Additional research is needed to examine this issue more fully as the role of inertia in online spaces is often debated,[125] and rarely measured with respect to various forms of cybercrime.[126]

Lastly, this study found substantive support for the role of target accessibility in shaping the risk of defacement by ideological actors compared to other motives for attack. Ideologically-motivated attackers were more likely to target homepages within websites and attack the same targets repeatedly. However, no significant relationships were observed between OS types and ideologically-motivated defacements. In terms of attack method, ideologically-motivated defacers were more likely to use unknown vulnerabilities and significantly less likely to use common attack methods compared to all other motives for defacements. These findings suggest ideological defacers may be less concerned with attacking targets of convenience than those who engage in defacements for more ego-centric motivations.

Taken as a whole, the findings of this study suggest that the target selection process of defacements stemming from ideological motivations were more purposive and designed to draw attention to causes using methods that reflect some degree of skill on the part of the attacker to effectively compromise a server.[127] Their efforts suggest defacers may be motivated by both subcultural values of the hacker subculture and broader situational values unique to the individual.[128] The preliminary nature of this study demonstrates the need for future research to assess how these dynamics persist across all forms of cyberattack for ideological motivations.[129] For instance, it is unclear what proportion of all hackers report engaging ideologically motivated attacks at some time.[130] Similarly, it is unknown whether those individuals who engage in ideologically expressive hacks more often construct their idenity as a hacker, and how that affects their proportional engagement in hacks for other reasons. Additionally, research is needed considering the extent to which target selection for cyberattacks differs on the basis of ideological alignment with far- left, far-right, jihadist, and single-issue agendas.[131]

It should be noted that this study utilized a very large data set, but one that is limited by self-reports provided by individuals who notify the Zone-H website. It is possible that the individuals who made the reports may not be the actual defacers, or that the notifiers may provide false information in order to conceal their true reasons for performing an attack. Further research is needed to more thoroughly

analyze the defacement content to determine how ideological attacks differ in substance or messaging from other motivations. A multi-method analysis could help overcome these challenges by combining qualitative and quantitative strategies to code the images, video, and text appearing in the defaced site to triangulate the extent to which the information provided corresponds with the motivation reported. Such strategies may be essential to clarify the nature of defacements by motive and validate the self-reported cause relative to language used in the attack text itself.[132]

Additionally, Zone-H reflects successful defacements rather than failed attacks which may limit the representative nature of the set generally. There is value in examining failed cyberattacks, as demonstrated by research considering both successful and failed plots of violent or criminal activities by extremist groups.[133] There is no easy way to catalog such incidents through open or closed channels due to the hidden nature of hacking. Researchers would benefit from direct engagement with active defacers using qualitative and quantitative methods to assess the frequency with which failure occurs, as well as foreground and situational factors that influence the likelihood of successfully defacing a target.[134]

Finally, this study focused solely on the U.S., which hosts a large amount of online content on servers within its physical borders. Future study is needed utilizing sites hosted in other nations to identify any potential variations that may be observed on the basis of attacker behavior. It is possible that Asian or European nations may experience attacks from ideological actors and groups that differ from those who may commonly target the U.S. It would be desirable for researchers to replicate this analysis using similar data sources to examine the relationship between target selection factors and motivation within a cross-national context. This would contribute to better identifying variations in attacker behavior relative to the physical and technological resources of nations around the world.

Notes

1. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York, NY: Oxford University Press, 2008); Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses* (London, UK: Routledge, 2016); David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, UK: Polity Press, 2007).
2. Benoit Dupont, Anne-Marie Cote, Jean-Ian Boutin, and Jose Fernandez, "Darkode: Recruitment Patterns and Transactional Features of 'The Most Dangerous Cybercrime Forum in the World'," *American Behavioral Scientist* 61, no. 11 (2017): 1219-43; Thomas J. Holt, "Subcultural Evolution? Examining the Influence of On-and Off-Line Experiences on Deviant Subcultures," *Deviant Behavior* 28, no. 2 (2007): 171-98; Rutger E. Leukfeldt, Edward R. Kleemans, and Wouter P. Stol, "Origin, Growth, and Criminal Capabilities of Cybercriminal Networks: An International Empirical Analysis," *Crime, Law and Social Change* 67, no. 1 (2017): 39-53; David Maimon, Amy Kamerdze, Michel Cukier, and Bertrand Sobesto, "Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective," *British Journal of Criminology* 53, no. 2 (2013): 319-43.
3. Scott H. Decker, "Exploring Victim-Offender Relationships in Homicide: The Role of Individual and Event Characteristics," *Justice Quarterly* 10, no. 4 (1993): 585-612; Jack Katz, *Seductions of Crime: Moral and Sensual Attractions in Doing Evil* (New York, NY: Basic Books, 1988).
4. Jason Franklin, Adrian Perrig, Vern Paxson, and Stefan Savage, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants" (Paper presented at ACM conference on Computer and Communications Security, Alexandria, Virginia, October 29 – November 2, 2007); Thomas J. Holt, Olga Smirnova, and Yi Ting Chua, "Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets," *Deviant Behavior* 37, no. 4 (2016): 353-67; Max Kilger, "Social Dynamics and the Future of Technology-Drive Crime," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell, (Hershey, PA: IGI Global, 2011), 205-27.
5. Dorothy E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell (Hershey, PA: IGI Global, 2011), 170-86; Thomas J. Holt, Joshua D. Freilich, and Steven M. Chermak, "Exploring the Subculture of Ideologically Motivated Cyber-Attackers," *Journal of Contemporary Criminal Justice* 33, no. 3 (2017): 212-33; Thomas J. Holt, Mattisen Stonhouse, Joshua D. Freilich, and Steven M. Chermak, "Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups," *Terrorism and Political Violence*, (2019): 1-22; Lee Jarvis and Stuart Macdonald, "Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon," *Perspectives on Terrorism* 8, no. 2 (2014): 52-65; Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (Abingdon, UK: Routledge, 2004).

6. Jarvis and Macdonald, "Locating Cyberterrorism."
7. Majid Yar, *Cybercrime and Society* (Thousand Oaks, CA: Sage, 2013).
8. Thomas J. Holt, Adam M. Bossler, and Sarah Fitzgerald, "Examining State and Local Law Enforcement Perceptions of Computer Crime," in *Crime On-Line: Correlates, Causes, and Context*, 2nd ed. (Durham, NC: Carolina Academic Press, 2010), 221-46; Jarvis and Macdonald, "Locating Cyberterrorism."
9. Department of Homeland Security, *Assessment: Leftwing Extremists Likely to Increase Use of Cyberattacks over the Coming Decade*(Washington, DC, 2010).
10. Thomas J. Holt, "Exploring the Intersections of Technology, Crime, and Terror," *Terrorism and Political Violence* 24, no. 2 (2012): 337-54; Jordan and Taylor, *Hacktivism and Cyberwars*; Yar, *Cybercrime and Society*.
11. Brenner, *Cyberthreats*; Wall, *Cybercrime.*
12. Joshua D. Freilich, Steven M. Chermak, and Joseph Simone Jr., "Surveying American State Police Agencies about Terrorism Threats, Terrorism Sources, and Terrorism Definitions," *Terrorism and Political Violence* 21, no. 3 (2009): 450-75; Joshua D. Freilich, Steven M. Chermak, Roberta Belli, Jeff Gruenewald, and William S. Parkin, "Introducing the United States Extremist Crime Database (ECDB)," *Terrorism and Political Violence* 26, no. 2 (2014): 372-84.
13. Holt and Bossler, *Cybercrime in Progress.*
14. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Hyun-Jin Woo, Yeora Kim, and Joseph Dominick, "Hackers: Militants or Merry Pranksters? A Content analysis of Defaced Web Pages," *Media Psychology* 6, no. 1 (2004): 63-82.
15. Holt, Freilich, and Chermak, "Exploring the subculture"; Kilger, "Social Dynamics"; Woo, Kim, and Dominick, "Hackers."
16. Woo, Kim, and Dominick, "Hackers."
17. *Ibid*.; H. Zone, "News," (2018), http://www.zone-h.org/news/id/4737 (accessed April 11, 2018).
18. Holt, "Subcultural Evolution"; Woo, Kim, and Dominick, "Hackers."
19. Holt, Freilich, and Chermak, "Exploring the Subculture"; Woo, Kim, and Dominick, "Hackers."
20. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
21. Hollie McKay, "Cause for Concern? Pro-ISIS Hacking Group Targets 800 US School Websites," *Fox News*, November 12, 2017, https://www.foxnews.com/tech/cause-for-concern-pro-isis-hacking-group-targets-800-us-school-websites (accessed December 1, 2017).
22. Stephen Brown, "Hackers Post Fascist Slogans on Nazi Camp Website," *Reuters*, July 28, 2010, https://www.reuters.com/article/us-germany-buchenwald-neonazis/hackers-post-facist-slogans-on-nazi-camp-website-idUSTRE66R4EG20100728 (accessed December 1, 2017).
23. Claude Berrebi and Darius Lakdawalla, "How does Terrorism Risk Vary Across Space and Time? An Analysis Based on the Israeli Experience," *Defense and Peace Economics* 18, no. 2 (2007): 113-31; Daphna Canetti-Nisim, Gustavo Mesch, and Ami Pedahzur, "Victimization from Terrorist Attacks: Randomness or Routine Activities?" *Terrorism and Political Violence* 18, no. 4 (2006): 485-501; Yariv Feniger and Ephraim Yuchtman-Yaar, "Risk Groups in Exposure to Terror: The Case of Israel's Citizens," *Social Forces* 88, no. 3 (2010): 1451-62; William S. Parkin, Joshua D. Freilich, and Steven M. Chermak, "Ideological Victimization: Homicides Perpetrated by Far-Right Extremists," *Homicide Studies* 19, no. 3 (2015): 211-36.
24. Holt and Bossler, *Cybercrime in Progress*; Ronald V. Clarke and Graeme R. Newman, *Superhighway Robbery: Preventing E-Commerce Crime* (Cullompton, UK: Willan Press, 2003).
25. Holt, Freilich, and Chermak, "Exploring the Subculture."
26. Thomas J. Holt and Max Kilger, "Examining Willingness to Attack Critical Infrastructure Online and Offline," *Crime & Delinquency* 58, no. 5 (2012): 798-822.
27. Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, (1979): 588-608.
28. William S. Parkin and Joshua D. Freilich, "Routine Activities and Right-Wing Extremists: An Empirical Comparison of the Victims of Ideologically-and non-Ideologically-Motivated Homicides Committed by American Far-Rightists," *Terrorism and Political Violence* 27, no. 1 (2015): 182-203; Parkin, Freilich, and Chermak, "Ideological Victimization."
29. Paolo Passeri, "August 2014 Cyber Attacks Statistics," *Hackmageddon*, March 14, 2015, http://hackmageddon.com/2014/09/08/august-2014-cyber-attacks-statistics/; Zone H, "News."
30. Holt, Freilich, and Chermak, "Exploring the Subculture"; Jordan and Taylor, *Hactivism and Cyberwars.*
31. Marco Balduzzi, Ryan Flores, Lion Gui, and Frederico Maggi, *A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks* (Trend Micro, 2018) https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf; Holt, Freilich, and Chermak, "Exploring the Subculture"; Thomas J. Holt, Rutger Leukfeldt, and Steve Van De Weijer, "An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites," *Criminal Justice and Behavior* (2020); C. Jordan Howell, George W. Burruss, David Maimon, and Shradha Sahani, "Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets," *Journal of Crime and Justice* 42, no. 5 (2019): 536-50; Jordan and Taylor, *Hactivism and Cyberwars*; Woo, Kim, and Dominick, "Hackers."

32. Holt and Bossler, *Cybercrime in Progress*; Holt, Smirnova, and Chua, "Exploring and Estimating the Revenues and Profits."
33. Katz, *Seductions of Crime.*
34. Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Holt, Freilich, and Chermak, "Exploring the Subculture"; Howell et al., "Website Defacement and Routine Activities"; Woo, Kim, and Dominick, "Hackers."
35. *Ibid.*
36. *Ibid.*
37. Kilger, "Social Dynamics."
38. Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Jordan and Taylor, *Hacktivism and Cyberwars*: Holt, Freilich, and Chermak, "Exploring the Subculture"; Woo, Kim, and Dominick, "Hackers."
39. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London, UK: Verso Books, 2014); Jordan and Taylor, *Hactivism and Cyberwars*; Erik Skare, "Digital Surveillance/Militant Resistance: Categorizing the "Proto-state Hacker." *Television & New Media* 20, no. 7 (2018): 670-85.
40. Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Jordan and Taylor, *Hacktivism and Cyberwars*: Denning, "Cyber Conflict."
41. Jordan and Taylor, *Hacktivism and Cyberwars.*
42. Denning, "Cyber Conflict"; Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Woo, Kim, and Dominick, "Hackers."
43. Denning, "Cyber Conflict."
44. *Ibid.*
45. Holt, Freilich, and Chermak, "Exploring the Subculture."
46. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
47. Brown, "Hackers Post Fascist Slogans"; Darlene Storm, "Political Hackers Attack Russia, Nazi Defacement, Threaten US CENTCOM with Cyberattack," *Computerworld*, March 3, 2014, https://www.computerworld.com/article/2476002/political-hackers-attack-russia–nazi-defacement–threaten-us-centcom-with-cybera.html.
48. Holt, Freilich, and Chermak, "Exploring the Subculture"; Woo, Kim, and Dominick, "Hackers."
49. Canetti-Nisim, Mesch, and Pedahzur, "Victimization from Terrorist Attacks"; Kelly R. Damphousse, Brent L. Smith, and Amy Sellers, "The Targets and Intended Victims of Terrorist Activities in the United States," in *Meeting the Challenges of Global Terrorism: Prevention, Control, and Recovery*, edited by Dilip K. Das and Peter C. Kratcoski (Lexington, KY: Lexington Books, 2002), 171-88.
50. Amy Adamczyk, Jeff Gruenewald, Steven M. Chermak, and Joshua D. Freilich, "The Relationship Between Hate Groups and Far-Right Ideological Violence," *Journal of Contemporary Criminal Justice* 30, no. 3 (2014): 310-32; Berrebi and Lakdawalla, "How Does Terrorism Risk Vary"; Canetti-Nisim, Mesch, and Pedahzur, "Victimization from Terrorist Attacks"; Donald P. Green, Dara Z. Strolovitch, and Janelle S. Wong, "Defended Neighborhoods, Integration, and Racially Motivated Crime," *American Journal of Sociology* 104, no. 2 (1998): 372-403; Parkin, Freilich, and Chermak, "Ideological Victimization."
51. Parkin, Freilich, and Chermak, "Ideological Victimization."
52. C. Puzzanchera, G. Chamberlin, and W. Kang, *Easy Access to the FBI's Supplementary Homicide Reports: 1980-2010* (Washington, DC: National Center for Juvenile Justice, 2012).
53. Parkin, Freilich, and Chermak, "Ideological Victimization."
54. *Ibid.*
55. Cohen and Felson, "Social Change."
56. Guy Griffiths, Shane D. Johnson, and Kevin Chetty, "UK-Based Terrorists' Antecedent Behavior: A Spatial and Temporal Analysis," *Applied Geography* 86 (2017): 274-82; Gary LaFree, Laura Dugan, Min Xie, and Piyusha Singh, "Spatial and Temporal Patterns of Terrorist Attacks by ETA 1970 to 2007," *Journal of Quantitative Criminology* 28, no. 1 (2012): 7-29; Kim D. Rossmo and Keith Harries, "The Geospatial Structure of Terrorist Cells," *Justice Quarterly* 28, no. 2 (2011): 221-48.
57. Rutger E. Leukfeldt and Majid Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," *Deviant Behavior* 37, no. 3 (2016): 263-80; Clarke and Newman, *Superhighway Robbery*; Majid Yar, "The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory," *European Journal of Criminology* 2, no. 4 (2005): 407-27.
58. Yar, "The Novelty of 'Cybercrime'."
59. Thomas J. Holt and Adam M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," *Deviant Behavior* 30, no. 1 (2008): 1-25; Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Catherine D. Marcum, George E. Higgins, Tina L. Freiburger, and Melissa L. Ricketts, "Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime," *International Journal of Police Science & Management* 12, no. 4 (2010): 516-25.
60. Adam M. Bossler and Thomas J. Holt, "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology* 3, no. 1 (2009): 400-20;

Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Maimon, Kamerdze, Cukier, and Sobesto, "Daily Trends and Origin."

61. Bossler and Holt, "On-Line Activities"; Kyung-Shick Choi, "Computer Crime Victimization and Integrated Theory: An Empirical Assessment," *International Journal of Cyber Criminology* 2, no. 1 (2008): 308-33.
62. Travis C. Pratt, Kristy Holtfreter, and Michael D. Reisig, "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory," *Journal of Research in Crime and Delinquency* 47, no. 3 (2010): 267-96; Fawn T. Ngo and Raymond Paternoster, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors," *International Journal of Cyber Criminology* 5, no. 1 (2011): 773-93.
63. Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Clarke and Newman, *Superhighway Robbery*.
64. Holt and Kilger, "Examining Willingness"; Jordan and Taylor, *Hacktivism and Cyberwars.*
65. Vasileios Karagiannopoulos, *Living With Hacktivism: From Conflict to Symbiosis* (Cham, Switzerland: Springer, 2018); Yar, "The Novelty of 'Cybercrime'."
66. Thomas J. Holt, George W. Burruss, and Adam M. Bossler, "Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework," *International Journal of Offender Therapy and Comparative Criminology* 62, no. 6 (2018): 1720-41.
67. Holt, Freilich, and Chermak, "Exploring the Subculture"; Jordan and Taylor, *Hacktivism and Cyberwars.*
68. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Jordan and Taylor, *Hacktivism and Cyberwars.*
69. Parkin, Freilich, and Chermak, "Ideological Victimization."
70. Brenner, *Cyberthreats;* Thomas Rid, *Cyber War Will Not Take Place* (New York, NY: Oxford University Press, 2013).
71. Marcus Felson, *Crime and Everyday Life* (Thousand Oaks, CA: Pine Forge Press, 1998); Yar, "The Novelty of 'Cybercrime'."
72. Felson, *Crime and Everyday Life*; Jordan and Taylor, *Hacktivism and Cyberwars*; Woo, Kim, and Dominick, "Hackers."
73. Parkin, Freilich, and Chermak, "Ideological Victimization."
74. Freilich, Chermak, Belli, Gruenewald, and Parkin, "Introducing the United States"; Parkin and Freilich, "Routine Activities."
75. Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Elsevier, 2013); Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime."
76. Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Paul Taylor, *Hackers: Crime and the Digital Sublime* (London, UK: Routledge, 2012).
77. Taylor, *Hackers.*
78. Andress and Winterfeld, *Cyber Warfare.*
79. Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime."
80. Holt, Freilich, and Chermak, "Exploring the Subculture."
81. *Ibid.*
82. Andress and Winterfeld, *Cyber Warfare.*
83. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Jordan and Taylor, *Hacktivism and Cyberwars.*
84. Holt, Freilich, and Chermak, "Exploring the Subculture"; Woo, Kim, and Dominick, "Hackers."
85. Holt, Freilich, and Chermak, "Exploring the Subculture"; Maimon, Kamerdze, Cukier, and Sobesto, "Daily Trends and Origin."
86. Jordan and Taylor, *Hacktivism and Cyberwars*; Maimon, Kamerdze, Cukier, and Sobesto, "Daily Trends and Origin"; David Maimon, Theodore Wilson, Wuling Ren, and Tamar Berenblum, "On the Relevance of Spatial and Temporal Dimensions in Assessing Computer Susceptibility to System Trespassing Incidents," *British Journal of Criminology* 55, no. 3 (2015): 615-34.
87. Parkin, Freilich, and Chermak, "Ideological Victimization."
88. Ronald V. G. Clarke and Graeme R. Newman, *Outsmarting the Terrorists* (New York, NY: Greenwood Publishing Group, 2006); Parkin, Freilich, and Chermak, "Ideological Victimization."
89. Holt, Freilich, and Chermak, "Exploring the Subculture"; Jordan and Taylor, *Hacktivism and Cyberwars.*
90. Andress and Winterfeld, *Cyber Warfare*; Taylor, *Hackers.*
91. Andress and Winterfeld, *Cyber Warfare*; Steven Furnell, *Cybercrime: Vandalizing the Information Society* (London: Addison-Wesley, 2002).
92. Thomas J. Holt, "Examining the Role of Technology in the Formation of Deviant Subcultures," *Social Science Computer Review* 28, no. 4 (2010): 466-81; Marleen Weulen Kranenbarg, Thomas J. Holt, and Jean-Louis van Gelder, "Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap," *Deviant Behavior* 40, no. 1 (2019): 40-55; Taylor, *Hackers.*

93. Andress and Winterfeld, *Cyber Warfare*; Weulen Kranenbarg, Holt, and van Gelder, "Offending and Victimization."
94. Taylor, *Hackers.*
95. Weulen Kranenbarg, Holt, and van Gelder, "Offending and Victimization."
96. Thomas J. Holt, "Examining the Forces Shaping Cybercrime Markets Online," *Social Science Computer Review* 31, no. 2 (2013): 165-77.
97. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Jordan and Taylor, *Hacktivism and Cyberwars.*
98. Holt, Freilich, and Chermak, "Examining the Subculture."
99. Andress and Winterfeld, *Cyber Warfare.*
100. Holt, "Subcultural Evolution"; Holt and Kilger, "Examining Willingness."
101. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Jordan and Taylor, *Hacktivism and Cyberwars*; Woo, Kim, and Dominick, "Hackers."
102. Freilich, Chermak, Belli, Gruenewald, and Parkin, "Introducing the United States"; Gary LaFree and Laura Dugan, "Research on Terrorism and Countering Terrorism," *Crime and Justice* 38, no. 1 (2009): 413-77.
103. Holt and Bossler, *Cybercrime in Progress*; Holt, Burruss, and Bossler, "Assessing the Macro-Level"; Wall, *Cybercrime.*
104. Brenner, *Cyberthreats;* Holt and Bossler, *Cybercrime in Progress*; Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks"; Wall, *Cybercrime.*
105. Dupont, Cote, Boutin, and Fernandez, "Darkode,"; Holt, Burruss, and Bossler, "Assessing the Macro-Level"; Leukfeldt, Kleemans, and Stol, "Origin, Growth, and Criminal Capabilities"; Maimon, Kamerdze, Cukier, and Sobesto, "Daily Trends and Origin."
106. Jordan and Taylor, *Hacktivism and Cyberwars*; Woo, Kim, and Dominick, "Hackers."
107. Zone, "News."
108. Woo, Kim, and Dominick, "Hackers."
109. Jennifer V. Carson, Gary LaFree, and Laura Dugan, "Terrorist and non-Terrorist Criminal Attacks by Radical Environmental and Animal Rights Groups in the United States, 1970-2007," *Terrorism and Political Violence* 24, no. 2 (2012): 295-319; Freilich, Chermak, Belli, Gruenewald, and Parkin, "Introducing the United States."
110. Woo, Kim, and Dominick, "Hackers."
111. Puzzanchera, Chamberlin, and Kang, "Easy Access."
112. Holt, "Subcultural Evolution"; Kevin F. Steinmetz, "Craft(y)ness: An Ethnographic Study of Hacking," *British Journal of Criminology* 55, no. 1 (2015): 125-45; Woo, Kim, and Dominick, "Hackers."
113. Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Holt, Leukfeldt, and van de Weijer, "An examination of motivation and routine activity theory."
114. *Ibid.*
115. Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Taylor, *Hackers.*
116. Holt, Freilich, and Chermak, "Exploring the Subculture."
117. As a sensitivity analysis, two separate binary logistic regression models were estimated for political and patriotically-motivated defacements. The findings demonstrate that political defacements were more likely to involve single defacements, target the homepage of websites, involve repeat attacks, and were more likely to involve undisclosed vulnerabilities, while less likely to involve both SQL injection and known vulnerabilities. Patriotic defacements were more likely to involve TLDs of foreign nations, affect linux systems, and were less likely to involve the use of known vulnerabilities. All of these items were significant in the regression model involving the combined measure for political and patriotic defacements, with one exception:.edu domains were non-significant in each individual model, though it was approaching significance (.07 and .08 respectively). Since this item was significant in the combined model, it is likely a reflection of increased statistical power achieved through a more conservative combined measure.
118. Parkin and Freilich, "Routine Activities"; Parkin, Freilich, and Chermak, "Ideological Victimization."
119. Cohen and Felson, "Social Change."
120. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
121. Adamczyk, Gruenewald, Chermak, and Freilich, "The Relationship Between Hate Groups"; Berrebi and Lakdawalla, "How Does Terrorism Risk Vary"; Canetti-Nisim, Mesch, and Pedahzur, "Victimization from Terrorist"; Green, Strolovitch, and Wong, "Defended Neighborhoods"; Parkin, Freilich, and Chermak, "Ideological Victimization."
122. Brenner, *Cyberthreats;* Rid, *Cyber War.*
123. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
124. Parkin and Freilich, "Routine Activities"; Parkin, Freilich, and Chermak, "Ideological Victimization."
125. Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime"; Yar, "The Novelty of 'Cybercrime'."
126. Holt and Bossler, *Cybercrime in Progress*; Leukfeldt and Yar, "Applying Routine Activity Theory to Cybercrime."
127. Holt, Freilich, and Chermak, "Examining the Subculture"; Weulen Kranenbarg, Holt, and van Gelder, "Offending and Victimization."

128. Balduzzi, Flores, Gui, and Maggi, *A Deep Dive into Defacement*; Holt "Subcultural evolution."
129. Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
130. Coleman, *Hacker, Hoaxer, Whistleblower, Spy*; Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks."
131. *Ibid.*
132. Holt, Freilich, and Chermak, "Exploring the Subculture."
133. Carson, LaFree, and Dugan, "Terrorist and non-Terrorist Criminal Attacks by Radical Environmental and Animal Rights Groups in the United States, 1970-2007"; Freilich, Chermak, Belli, Gruenewald, and Parkin, "Introducing the United States."
134. Holt, Freilich, and Chermak, "Exploring the Subculture."

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the U.S. Department of Homeland Security [ASUB00000368].

Notes on contributors

Thomas J. Holt is a professor in and director of the School of Criminal Justice at Michigan State University. His research focuses on cybercrime, cyberterrorism, and the policy response to these issues.

Jin Ree Lee is a PhD student in the School of Criminal Justice at Michigan State University. His research focuses on cybercrime and testing criminological frameworks to understand these phenomena.

Joshua D. Freilich is a professor in the Criminal Justice Department and the Criminal Justice PhD Program at John Jay College. He is the Creator and co-Director of the United States Extremist Crime Database (ECDB), an open source relational database of violent and financial crimes committed by political extremists in the U.S. Professor Freilich's research has been funded by the Department of Homeland Security (DHS) and the National Institute of Justice (NIJ).

Steven M. Chermak is a professor in the School of Criminal Justice at Michigan State University. Dr. Chermak is interested in studying terrorism, school shootings, mass shootings, criminal justice organizations, and media coverage of crime and criminal justice. Much of his work in the last ten years has focused on terrorist and extremist activity.

Johannes M. Bauer is the Quello Chair in Media and Information Policy and Chairperson of the Department of Media and Information, is a researcher, writer, teacher, and academic entrepreneur. His ongoing research focuses on innovation in the next-generation Internet (Internet of Things, 5G wireless), digital entrepreneurship (both for-profit and social), and governance challenges.

Ruth Shillair is an assistant professor in the Department of Media and Informatics at Michigan State University. Her research considers the human aspects of Cybersecurity, the impacts of security and digital literacy on different age groups, improving cybersecurity education, and increasing cybersecurity capacity.

Arun Ross, the John and Eva Cillag Endowed Chair in Science and Engineering, is a professor in the Department of Computer Science and Engineering. Ross is an internationally recognized expert in biometrics, computer vision, and machine learning.